Chapter 3

The Secretary of State's Office Should Improve Controls Over Access to the TEAM System

Auditors identified weaknesses associated with controls over the TEAM system that increase the risk of unauthorized access to voter data. However, auditors did not identify any instances in which data was inappropriately accessed or modified.

Chapter 3-A

The Secretary of State's Office Does Not Have Adequate Controls Over User Access to the TEAM Application and Database

Specific control weaknesses over user access to the TEAM system increase the risk of unauthorized access to voter data. Specifically:

- The Secretary of State's Office delegated the responsibility for setting up county user access accounts to county administrators without properly training the administrators. In addition, the Secretary of State's Office also gave county administrators the ability to delegate their access rights to other users. As a result, some county administrators had granted administrative access rights to the TEAM system to most, if not all, the TEAM system user accounts in their counties. Auditors determined that county administrators granted administrative access to 111 (54 percent) of the 204 county user accounts tested. In 8 (24 percent) of the 33 counties represented in the test sample, county administrators gave administrative access to all TEAM system user accounts in their counties. Administrative access gives users extensive access to the TEAM system and allows users to make widespread changes to a county's voter registration data.

- The Secretary of State's Office could not confirm whether any of the TEAM system user accounts in the county voter registration offices and one other user account had been assigned to actual employees. In addition, 9 (4.4 percent) of 204 county user accounts tested appeared to be group accounts and did not have an individual's name attached to them. Auditors also determined that 13 percent of state administrative access accounts were test accounts, and the Secretary of State's Office could not determine whether these accounts were being used. As a result, the Secretary of State's Office would not be able to identify the specific individual who used one of these accounts to make inappropriate changes to TEAM system data. The Secretary of State's Office's account management policy requires that all accounts be uniquely identifiable and use an assigned user name.

- The Secretary of State's Office did not have a formal process for reviewing the validity of existing users' accounts or for closing terminated

users' accounts. As a result, auditors determined that four users in two county voter registration offices that auditors visited were not current county employees. Because auditors visited only 11 counties, additional examples of this weakness may exist at the other 243 counties not visited. The Secretary of State's Office's account management policy requires that system administrators or other designated staff have a documented process for periodically reviewing existing accounts for validity.

- Although the Secretary of State's Office collected TEAM access logs, it had not implemented automated tools to allow it to regularly analyze the voluminous data collected. Title 1, Texas Administration Code, Section 202.25, requires that all information resource systems provide the means by which management can audit information system records and establish individual accountability for any action that can potentially allow access to, generation of, modification of, or allow the release of confidential information. Without automated tools to analyze the voluminous audit log data collected and to assist in identifying trends that may indicate security breaches, the Secretary of State's Office may not detect and prevent unauthorized user access or unauthorized changes to TEAM system data.

- The Secretary of State's Office had appropriate controls in place to prevent access to the TEAM database by unauthorized users without direct access to the database. For example, all security-critical default accounts had been disabled. However, auditors determined that certain direct database access and security controls can be improved. To minimize the risk of a security breach, auditors communicated in writing details about these control weaknesses directly to the Secretary of State's Office.

Responses to the survey auditors sent to county voter registration offices underscored these findings. Specifically:

- 26 (13 percent) of the 207 offices that answered the question, "Do multiple users share the same log-in account(s) in the TEAM system?" answered "Yes."

- 35 (17 percent) of the 203 offices that answered the question, "Did everyone who had access to the TEAM system sign an Information Security Acknowledgement and Non-disclosure Agreement (ISANA) form?" answered "No." Another 27 (13 percent) offices stated they did not know of the ISANA form. The Secretary of State's Office's account management policy requires that all users must sign the ISANA form before access is given to the TEAM system. There is a risk that users who do not sign the ISANA form may disclose private, confidential, or high-risk information to unauthorized parties.

Recommendations

The Secretary of State's Office should:

- Require formal access request forms be submitted to the TEAM security administrator for all TEAM users, including county users and contractors.
- Limit the ability of county administrators to delegate TEAM administrator roles to other county users.
- Ensure all users have read and signed the ISANA form.
- Review all existing county, Secretary of State's Office employee, and contractor accounts and remove or modify those accounts that are not appropriately assigned.
- Establish and implement procedures for periodically reviewing existing accounts for validity.
- Remove test user access accounts with administrative access to the TEAM system.
- Develop an automated process for monitoring and analyzing audit log data and develop standards and procedures for regular review of access logs.

Management's Response

Management agrees with these recommendations. The Office's Information Security Officer will work closely with the Office's Elections division to address these recommendations. Specifically, the Office will review its current request forms, make any necessary modifications to these forms and ensure that the proper forms are submitted to the Secretary of State's Office by the counties. The Office will also meet with the vendor and explore the feasibility of installing additional security controls within TEAM, and then associating those controls with the primary role of the end-user. Similarly, the Office will develop processes to monitor county compliance with SOS security policies, including and especially the Information Security Acknowledgment and Non-Disclosure Agreement.

Additionally, the Office will work with the counties and implement procedures so that county accounts can be reviewed for validity and proper authority levels can be ascertained. The Office will also investigate the use of log analysis tools to aid in reviewing access logs.

Finally, the Office of the Secretary of State has developed a process whereby the Office can ascertain what accounts exist, and to whom these accounts have been assigned within the Office and each particular county. The process that has been developed is currently a manual one, and the Office is working

to make this process an automated one. Test user accounts have been eliminated from the TEAM system.

Chapter 3-B

The Secretary of State's Office Has Inadequate Change Management Procedures for the TEAM System

The Secretary of State's Office does not follow a consistent change management process for the TEAM system. Some change requests were made directly by the development staff using e-mails. If no one on the Technical Infrastructure Committee (the members of which are on the change request's e-mail distribution list) questioned the change, then programmers made the change themselves and sometimes communicated completion of the change to the committee using e-mail. These e-mails did not show whether requests were approved or whether changes were tested.

In addition, these changes were not recorded on a change request log as required by Secretary of State's Office policy. Only changes questioned by a member of the Technical Infrastructure Committee are submitted to the Secretary of State's Office's Change Control Board, which is responsible for changes to the TEAM system. The Secretary of State's Office could provide auditors only one change request that had been submitted to its Change Control Board. The Secretary of State's Office could not provide documentation to auditors showing change request approvals, back-out plans, test results, and system documentation updates for any changes, including emergency changes. The Secretary of State's Office's change management policy requires that such documentation be maintained.

System programmers and others applying changes directly to the production environment without testing these changes could cause data corruption, system crashes, and related problems. In addition, the lack of a formal, standardized process for managing changes to the TEAM system increases the risk that unauthorized changes could be made to applications and data without detection.

Recommendations

The Secretary of State's Office should establish and implement formal procedures to ensure that:

- Adequate documentation of decisions related to all change requests, such as prioritization and assignment of responsibilities, is maintained.
- All change requests are submitted using formal change request forms and that all users and approvers provide sign-offs on the forms.

- All emergency changes are logged, reviewed, and approved by management.
- All changes are tested and reviewed before implementation and all test and review documentation is maintained.
- Formal, detailed back-out instructions are drawn up for each change.
- System documentation is updated after every system change.

Management's Response

Management agrees with these recommendations. The SOS Information Technology Director will develop the necessary methodologies, documentation, forms and instructions to ensure that change management procedures are enhanced and that each of these recommendations are satisfied.

Chapter 3-C

Vulnerabilities Exist within the Secretary of State's Office Network

The Secretary of State's Office had secured the TEAM server and Web application from unauthorized access from outside the network. However, the Office had not secured other parts of its network from inappropriate access by individuals inside the Secretary of State's Office.

The TEAM server and Web application were secure.

Auditors reviewed the results of security scans performed by the Department of Information Resources that included the following:

- A penetration test conducted on October 30, 2006, of the servers on which the TEAM system runs. During this test, Department of Information Resources employees attempted to gain access to protected files in the Secretary of State Office's network.
- An application scan conducted on July 19, 2007, of the software on which the TEAM system runs. During this scan, the Department of Information Resources used an automated tool to search for vulnerabilities in the software.

The penetration test and the application scan did not identify any high-severity vulnerabilities that would negatively affect the security of the TEAM system. This means that TEAM servers and software did not have any weaknesses that could be used to easily access the system or take it off-line. However these test results do not provide a guarantee that the TEAM system will remain secure from unauthorized access attempts in the future.

The Secretary of State's Office has not corrected all vulnerabilities identified in a network scan performed by auditors.

As of September 10, 2007, the Secretary of State's Office had addressed only 6 (24 percent) of 25 high-severity vulnerabilities that were identified by a scan of the Secretary of State's Office's network that auditors performed on July 19, 2007. During the scan, auditors used an automated tool to identify the vulnerabilities of the Secretary of State's Office's network that present security risks of unauthorized access from inside the Secretary of State's Office.

The Secretary of State's Office did not have an active intrusion detection system.

The Secretary of State's Office did not have an intrusion detection system at the start of this audit. However, the Secretary of State's Office implemented an intrusion detection system during the scope of this audit. As a result, the Secretary of State's Office can now review access attempt logs, including firewall logs, and identify and address anomalies that could pose security threats to the TEAM system.

Recommendation

The Secretary of State's Office should address all high-severity vulnerabilities identified by the auditors' scan of the Secretary of State's Office's network.

Management's Response

Management agrees with this recommendation and has taken corrective action with respect to the 19 vulnerabilities that were identified as of September 10, 2007, but not corrected as of that date. The corrective action that was taken on these 19 vulnerabilities means that each of the 25 vulnerabilities that were identified by a scan of the Secretary of State's network by the State Auditor's Office on July 19, 2007 has been addressed and remediated.

Chapter 3-D

The Secretary of State's Office Does Not Have a Process in Place to Routinely Verify Data Backups

The Secretary of State's Office has a well established data backup schedule and stores backup media containing critical TEAM system data off site in a secure, environmentally safe, locked facility. However, the Secretary of State's Office does not have a process to routinely verify data backups; such a process is required by the Secretary of State's Office's backup/disaster recovery policy. Without a process to verify data backups, the Secretary of

State's Office may not be aware that an unsuccessful or unreadable backup has been made and would be unable to maintain or quickly resume mission-critical functions in a disaster.

Recommendation

The Secretary of State's Office should establish a process to routinely verify data backups.

Management's Response

Management agrees with this recommendation. The service provider for operational support of the SOS data center environment is the Texas Department of Information Resources (DIR) as per the statewide data consolidation project currently underway. The SOS has been working with DIR to make sure that DIR and its partner in the data consolidation endeavor, the "Team for Texas" (which is a team of vendors headed up by IBM), are performing routine verification of data backups.

Appendices

Appendix 1

Objectives, Scope, and Methodology

Objectives

The objectives of this audit were to:

- Determine whether the records in the statewide voter registration database are accurate in accordance with the Help America Vote Act of 2002.
- Assess whether the statewide voter registration system will be available when needed.
- Determine whether the Web-based statewide voter registration system is protected from unauthorized access.

Scope

The scope of this audit included the voter registration component of the Texas Election Administration Management (TEAM) system and the processes and controls at the Secretary of State's Office and county voter registration offices, which coordinated with each other to generate a list of voters who were eligible to vote during the May 12, 2007, special election.

Methodology

The audit methodology included interviewing Secretary of State's Office personnel; interviewing election staff and information technology staff at 11 selected county voter registration offices; reviewing Secretary of State's Office documentation; analyzing TEAM system data and configurations; testing voter registration records for eligibility; reviewing processes, policies, and procedures for determining voter eligibility; and conducting security scans of the Secretary of State's Office network. Auditors also surveyed 254 county voter registration offices regarding the use of the TEAM system as of August 3, 2007.

Information collected and reviewed included the following:

- Secretary of State's Office policies and procedures.
- TEAM voter registration data.
- TEAM user account information, configuration documents, and implementation documents.
- Bureau of Vital Statistics death records through November 30, 2007.

- Department of Criminal Justice report of persons serving felony sentences in May 2007, including those who were incarcerated, serving parole, or on probation.
- Department of Information Resources penetration test summaries and application scan reports.
- Computer systems and networks at selected county voter registration offices.

Procedures and tests conducted included the following:

- Conducted interviews with key staff from the Secretary of State's Office and county voter registration offices regarding the TEAM system.
- Analyzed voter registration data from the TEAM system.
- Tested voting history of registrants who may not have been eligible for the May 12, 2007, special election.
- Analyzed TEAM system data and controls.
- Tested user accounts in the TEAM system for appropriateness.
- Physically inspected the data center and servers that run the TEAM system.
- Scanned the Secretary of State's Office's computer network for security weaknesses.
- Surveyed county voter registration offices.

Criteria used included the following:

- Title 42, United States Code, Section 15301 (Help America Vote Act of 2002).
- Title 1, Texas Election Code, Chapters 11 through 18.
- Title 42, United States Code, Section 1973 (National Voter Registration Act of 1993).
- Title 1, Texas Administrative Code, Chapter 81.
- Title 1, Texas Administrative Code, Chapter 202.
- Secretary of State's Office's contract with IBM for the development of the TEAM system.
- Secretary of State's Office's policies and procedures.

- Department of Information Resources guidelines.

Project Information

Audit fieldwork was conducted from May 2007 through September 2007. This audit was conducted in accordance with generally accepted government auditing standards.

The following members of the State Auditor's staff performed the audit:

- Kels Farmer, CISA (Project Manager)
- Joseph Mungai, CIA, CISA (Assistant Project Manager)
- Hillary Hornberger, CIA
- Alexis Markham
- Robert Pagenkopf
- Stacy Snoe
- Cody Tubbs
- Wei Wang, MSAS, CPA, CIA, CISA
- Rachelle Wood, MBA
- Marlen Kraemer, MBA, CISA (Information System Audit Team)
- Serra Tamur, MPAff, CIA, CISA (Information System Audit Team)
- J. Scott Killingsworth, CIA, CGFM (Quality Control Reviewer)
- Michael C. Apperley, CPA (Assistant State Auditor)

Appendix 2

The U.S. Social Security Administration's Response to the State Auditor's Office's Request for Citizenship Data

Auditors contacted the U.S. Social Security Administration to obtain the United States citizenship status of registered voters in Texas; the U.S. Social Security Administration denied the request. Below is the text of the response that a program analyst in the Center for Program Support at the U.S. Social Security Administration e-mailed to Mr. Kels Farmer (the project manager overseeing this audit) on July 19, 2007:

Mr. Farmer,

The Social Security Administration (SSA) can only disclose personally identifiable information (PII) from its records without the individual's consent to various entities (including state and federal agencies) when there is legal authority via the Privacy Act and SSA disclosure regulates to do so. Your request does not meet the criteria so consent would be required. Additionally, SSA may not have current data on citizenship in all cases since individuals are not required to report back to SSA when citizenship status changes.

I hope this information is helpful.

Center for Program Support

U.S. Social Security Administration

Appendix 3

Texas Voter Registration Application

Figure 1

Texas Voter Registration Application

Texas Voter Registration Application

Prescribed by the Office of the Secretary of State

Complete These Questions Before Proceeding

Check one ☐ New ☐ Change ☐ Replacement

Are you a United States Citizen? ☐ Yes ☐ No

Will you be 18 years of age on or before election day? ☐ Yes ☐ No

If you checked 'no' in response to either of the above, do not complete this form.

Are you interested in serving as an election worker? ☐ Yes ☐ No

Answer below to complete application

Last Name	First Name	Middle Name (If any)	Former Name

Residence Address: Street Address and Apartment Number, City, State, and ZIP Code. If none, describe where you live. (Do not include P.O. Box or Rural Rt.)

Mailing Address: Street Address and Apartment Number or P.O. Box, City, State and ZIP Code. If mail cannot be delivered to your residence address.

Date of Birth: month, day, year

Gender (Optional) ☐ Male ☐ Female

TX Driver's License No. or Personal I.D. No. (issued by the Department of Public Safety)

☐ Check if you do not have a TX Driver's License, or Personal Identification Number

If no TX Driver's License or Personal Identification, give last 4 digits of your Social Security Number

☐ Check if you do not have a Social Security Number

Telephone Number, Include Area Code (Optional)

I understand that giving false information to procure a voter registration is perjury, and a crime under state and federal law. Conviction of this crime may result in imprisonment up to 180 days, a fine up to $2,000, or both.

I affirm that I

- am a resident of this county;
- have not been finally convicted of a felony or if a felon I have completed all of my punishment including any term of incarceration, parole, supervision, period of probation, or I have been pardoned; and
- have not been declared mentally incompetent by final judgment of a court of law.

X _____ Date

Signature of Applicant or Agent and Relationship to Applicant or Printed Name of Applicant if Signed by Witness and Date.

Qualifications

- You must register to vote in the county in which you reside.
- You must be a citizen of the United States.
- You must be at least 17 years and 10 months old to register, and you must be 18 years of age by election day.
- You must not be finally convicted of a felony, or if you are a felon, you must have completed all of your punishment, including any term of incarceration, parole, supervision, period of probation, or you must have received a pardon.

General Information

- Your voter registration will become effective 30 days after it is received or on your 18th birthday, whichever is later.
- If you move to another county, you must re-register in the county of your new residence.
- If you decline to register to vote, the fact that you have declined to register will remain confidential and will be used only for registration purposes. If you do register to vote, the identity of the office (if applicable) at which you submitted a voter registration application will remain confidential and will be used only for voter registration purposes.
- You must provide your Texas driver's license or personal identification number. If you do not have a driver's license or personal identification number, then give the last four digits of your social security number or if you do not have any of these identification numbers, then you must indicate by checking the appropriate box on the application side.

Identification Requirement

If you do not have a Texas driver's license or a social security number, you will be required to present identification when you vote in person or enclose a copy of such identification with your ballot if you vote by mail. Instead, you may enclose a copy of one of the following with this voter registration application. Identification includes: a current and valid ID; a copy of a current utility bill; bank statement; government check; paycheck; or other government document that shows your name and address.

Please complete sections by printing legibly. If you have any questions about how to fill out this application, please call your local voter registrar or the Secretary of State's Office toll free at 1-800-252-VOTE(8683).
TDD 1-800-735-2989. www.sos.state.tx.us.

Este formulario está disponible en Español. Favor de llamar sin cargo a la oficina del Secretario de Estado al 1-800-252-8683 para conseguir una versión en Español.

Appendix 4

County Voter Registration Offices That Maintain Their Own Voter Registration Databases

Table 2 lists the 30 counties that maintain their own voter registration databases and upload new registration records and changes to the Texas Election Administration Management (TEAM) system every 24 hours for verification.

Table 2

County Voter Registration Offices That Have Their Own Voter Registration Databases	
County Voter Registration Office	Number of Registered Voters [1]
Harris County	1,777,312
Dallas County	1,099,797
Bexar County	851,963
Travis County	524,689
Collin County	366,750
El Paso County	363,483
Denton County	318,501
Fort Bend County	258,408
Montgomery County	218,414
Williamson County	198,109
Cameron County	162,679
Jefferson County	145,191
Bell County	140,616
McLennan County	125,972
Smith County	119,777
Webb County	97,577
Wichita County	79,201
Ector County	65,488
Guadalupe County	65,175
Tom Green County	65,108
Kaufman County	53,381
Rockwall County	39,046
Bastrop County	37,459
Kerr County	32,444
Val Verde County	26,885
Fayette County	14,952
Grimes County	13,514
Morris County	8,936

County Voter Registration Offices That Have Their Own Voter Registration Databases	
County Voter Registration Office	Number of Registered Voters [a]
Terry County	7,086
Motley County	905

[a] Reflects status of county voter registration offices and number of voters per county as of May 2007.

Appendix 5

Survey Instruments and Results

The State Auditor's Office sent surveys to each of the 254 county voter registration offices in Texas asking about their experiences using the Texas Election Administration Management (TEAM) system. Auditors received 209 survey responses on or before August 3, 2007. Some offices elected not to answer all questions. Table 3 summarizes the responses.

Table 3

Survey Responses			
Question	Response	Number of Respondents	Percentage of Respondents
Do you have procedures to identify ineligible voter applicants, such as felons, non-citizens, or voters who submitted duplicate registrations?	Yes	89	43%
	No	96	46%
	Did not answer	24	11%
	Totals	209	100%
How often, if at all, do you find errors in the registered voter roll obtained from the Secretary of State's Office?	All the time	10	5%
	Often	30	14%
	Sometimes	73	35%
	Rarely	57	27%
	Never	16	8%
	Did not answer	23	11%
	Totals	209	100%
Do multiple users share the same log-in account(s) in the TEAM system?	Yes	26	12%
	No	181	87%
	Did not answer	2	1%
	Totals	209	100%
Did everyone who had to access the TEAM system sign an Information Security Acknowledgement and Non-disclosure Agreement (ISANA) form?	Yes	133	64%
	No	35	17%
	Other	35	17%
	Did not answer	6	3%
	Totals	209	100%
What kind of Internet connection do you use to access the TEAM system?	T1/T3 (Typical Speed: 100mps)	47	22%
	Cable/DSL (Typical Speed: 10mps)	118	56%
	Dial-up (Typical Speed: 56kbs)	4	2%
	Other	26	12%
	Did not answer	14	7%
	Totals	209	100%

Survey Responses			
Question	Response	Number of Respondents	Percentage of Respondents *
How often is TEAM available when you need to access the system?	Always	62	30%
	75% of the time or more	102	49%
	50% of the time or more	21	10%
	Less than 50% of the time	4	2%
	Less than 25% of the time	1	0%
	Other	18	9%
	Did not answer	1	0%
	Totals	209	100%
Is your county an online or offline county?	Online	183	88%
	Offline	25	12%
	Did not answer	1	0%
	Totals	209	100%
How quickly, on average, can the TEAM system process an online voter registration?	Less than 1 minute	19	9%
	1-2 minutes	55	26%
	3-5 minutes	45	22%
	6-10 minutes	28	13%
	More than 10 minutes	11	5%
	Other	25	12%
	Did not answer	26	12%
	Totals	209	100%
How quickly, on average, can the TEAM system generate a report?	Less than 1 hour	55	26%
	Less than 8 hours	61	29%
	Less than 24 hours	15	7%
	1-2 days	21	10%
	3-5 days	6	3%
	Other	24	11%
	Did not answer	27	13%
	Totals	209	100%
How satisfied are you with the TEAM system's ability to generate customized reports?	Very satisfied	6	3%
	Somewhat satisfied	37	18%
	Neutral	41	20%
	Not very satisfied	61	29%
	Very unsatisfied	33	16%
	Did not answer	31	15%
	Total	209	100%
Does the TEAM system process offline batch transactions in a timely manner?	Always	9	4%
	Often	12	6%
	Sometimes	4	2%

Survey Responses			
Question	Response	Number of Respondents	Percentage of Respondents
	Rarely	2	1%
	Never	1	1%
	Did not answer	181	87%
	Totals	209	100%
How quickly, on average, does the TEAM system process "send/receive" batched voter registration files?	Less than 1 minute	3	1%
	1-2 minutes	10	5%
	3-5 minutes	7	3%
	6-10 minutes	2	1%
	More than 10 minutes	0	0%
	Other	5	2%
	Did not answer	182	87%
	Totals	209	100%
How quickly, on average, can the TEAM system process a search for a voter?	Less than a minute	49	23%
	1-2 minutes	74	35%
	3-5 minutes	35	17%
	6-10 minutes	9	4%
	More than 10 minutes	2	1%
	Other	25	12%
	Did not answer	15	7%
	Totals	209	100%
How satisfied are you with the TEAM Help Desk Support?	Very satisfied	81	40%
	Somewhat satisfied	61	30%
	Neutral	27	13%
	Not very satisfied	19	9%
	Very unsatisfied	6	3%
	Do not use Help Desk Support	10	5%
	Did not answer	5	2%
	Totals	204	100%
Did you receive training from the Secretary of State's Office on the Team system?	Yes	194	93%
	No	15	7%
	Did not answer	0	0%
	Totals	209	100%
(If received training) To what extent did you find the training helpful?	To a great extent	23	12%
	To a good extent	68	35%
	To some extent	73	38%
	To a small extent	30	15%
	Not helpful at all	0	0%

Survey Responses			
Question	Response	Number of Respondents	Percentage of Respondents [a]
	Did not answer	15	8%
	Totals	194	100%
In general, does the TEAM system allow you to do your job effectively?	Yes	98	47%
	No	106	51%
	Did not answer	5	2%
	Totals	209	100%

[a] Percentages calculated in this table include offices that did not answer each question.

In addition, auditors asked county voter registration offices to list the most common problems they have encountered using the TEAM system, if any. Respondents could state up to five problems in response to this question. Auditors grouped similar responses, and the ten most common responses are listed in Table 4.

Table 4

Most Common Problems with the TEAM System Cited by County Voter Registration Offices	
Problem	Number of Respondents Listing Problem
The TEAM system is slow when processing new applications, setting up elections, generating reports, and generating voter rolls.	84
The TEAM system requires too many steps to do one task.	73
County voter registration staff have experienced difficulty running reports.	58
The street index—a feature of the TEAM system that assigns voting districts based on a voter's address—is complex, confusing, difficult, and time-consuming to edit.	56
The TEAM system times out often and will log users out.	41
The TEAM system is too difficult to use and not user-friendly. The previous voter registration system—Texas Voter Registration System (TVRS)—performed better and quicker.	41
County voter registration staff have experienced printing problems, such as the printer alignment not being correct and the system being unable to print three voter cards on one page (which the TEAM system was designed to do).	35
County voter registration staff could not get voter lists when needed (and did not want to set up an election to get them).	32
County voter registration staff need more training on the TEAM system; the manual provided by the Secretary of State's Office should be updated with more detailed, step-by-step instructions.	22
County voter registration staff experienced difficulty batching; the "create batch" button did not work.	20

Appendix 6

Secretary of State's Office's Attachment to Management Responses

The Secretary of State's Office provided this information as an attachment to its responses, which has not been subjected to any audit procedures.

Attachment A

The State of Texas

Elections Division
P.O. Box 12060
Austin, Texas 78711-2060
www.sos.state.tx.us

Phone: 512-463-5650
Fax: 512-475-2811
Dial 7-1-1 For Relay Services
(800) 252-VOTE (8683)

Phil Wilson
Secretary of State

As part of the Validation Activity, the TEAM Benchmark from December 2006 was rerun in order to document and compare the impact of the 6 months of tuning efforts. The follow summary shows the results for the original TEAM November 2006 benchmark (TEAM A and TEAM B), and the August 2007 (TEAM07) benchmark. In all cases, performance has significantly improved from the November 2006 Benchmark:

Test ID	Statistic	TEAM A	TEAM B	TEAM07	Faster by x
3.1.3 ADD	count	20	20	20	
	average	11.30	9.17	1.97	4.7
	stdev	7.59	6.20	0.84	
	confidence	3.33	2.72	0.37	
	maximum	25.39	18.35	3.88	4.7
	minimum	1.96	1.60	1.39	1.2
	correl				
	rec / sec				
3.2.2 CANCEL	count	13	12	14	
	average	5.83	4.79	1.83	2.6
	stdev	0.32	0.35	0.15	
	confidence	0.17	0.20	0.08	
	maximum	6.33	5.35	2.29	2.3
	minimum	5.08	4.28	1.66	2.6
	correl				
	rec / sec				
3.3.1 EDIT	count	14	15	14	
	average	7.93	4.17	1.91	2.2
	stdev	4.88	1.26	0.38	
	confidence	2.56	0.64	0.20	
	maximum	19.53	6.54	2.57	2.5
	minimum	4.09	2.19	1.50	1.5
	correl				
	rec / sec				
3.4.1 NAME	count	18	10	10	
	average	47.73	8.66	1.37	6.3
	stdev	130.66	12.77	0.20	
	confidence	60.36	7.92	0.12	

	maximum	541.74	43.99	1.86	23.6
	minimum	1.54	1.81	1.21	1.5
	correl	0.25	0.91	0.95	
	rec / sec	1.43	2.61	15.94	
3.4.2 VUID	count	22	10	10	
	average	2.76	2.39	1.26	1.9
	stdev	0.71	0.20	0.12	
	confidence	0.30	0.12	0.07	
	maximum	4.99	2.69	1.56	1.7
	minimum	1.45	2.08	1.14	1.8
	correl				
	rec / sec				
3.4.3 DOB	count	19	13	13	
	average	2.56	76.57	1.47	52.0
	stdev	1.15	187.07	0.17	
	confidence	0.52	101.69	0.09	
	maximum	5.01	692.87	1.80	385.4
	minimum	1.33	2.13	1.27	1.7
	correl				
	rec / sec				
Test ID	Statistic	TEAM A	TEAM B		
3.4.4 ADDR	count	10	10	10	
	average	2.94	12.85	1.54	8.4
	stdev	2.00	16.67	0.34	
	confidence	1.24	10.33	0.21	
	maximum	7.18	58.06	2.20	26.4
	minimum	1.38	0.74	1.13	0.7
	correl	0.96	0.59	0.95	
	rec / sec	8.00	4.38	33.52	
3.4.6 TDL	count	10	9	9	
	average	2.16	2.25	1.31	1.7
	stdev	0.61	0.24	0.04	
	confidence	0.36	0.16	0.03	
	maximum	2.94	2.81	1.37	2.1
	minimum	1.38	2.04	1.26	1.6
	correl				
	rec / sec				

2

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable David Dewhurst, Lieutenant Governor, Joint Chair
The Honorable Tom Craddick, Speaker of the House, Joint Chair
The Honorable Steve Ogden, Senate Finance Committee
The Honorable Thomas "Tommy" Williams, Member, Texas Senate
The Honorable Warren Chisum, House Appropriations Committee
The Honorable Jim Keffer, House Ways and Means Committee

Office of the Governor

The Honorable Rick Perry, Governor

Secretary of State

The Honorable Phil Wilson